Income Security Program (ISP)
Data Matching/Sharing - Security of Information & Privacy

Policy Guidelines and Audit Framework

In February of 1998 a review of all agreements ISP currently has concerning the sharing of information with the provinces and other federal agencies and programs was conducted. In all instances, it was reported that only those elements of personal information that must be disclosed in accordance with the relevant authority to do so was in fact given. Furthermore, in no cases was a complete copy of the databases provided.

The TB manual for Privacy and Data Protection volume provides a set of guidelines for the sharing of data and data matching programs. Benefits could be derived from developing a policy which will document what information may be shared and under what circumstances. Such a policy would help safeguard the personal information under ISPs control, at the same time such the policies and subsequent agreements would provide a framework which would enable a compliance audit to be conducted should one be required.

For the purpose of this document:

Data - is a set or sets of records containing information

Matching Program - is a specific procedure that is developed and used to compare data from one institution with data from another.

Information - is the product generated by a matching program

Policy with Respect to an Audit Framework

Internal Issues for ISP:

- The creation of a data dictionary which indicates each unique data field in all of ISPs systems and databases would be a useful resource for future agreements. For optimum benefit the data obtained from other government departments such as Canada Customs and Revenue Agency should also be included in the dictionary. Information of use in such a dictionary would be who the owner of the data is, which data elements may be shared, to whom and under what circumstances. For example, a case may arise that if a particular data element is identified as being sharable then in so choosing that item you may cause another sharable item to become non sharable. In other words, data items A and B are both sharable, however both A and B cannot be shared in the same match program. This dictionary could prove to be a useful tool in an audit.

- It is the policy of the government to prevent the SIN from becoming a universal identifier. However, provincial governments have been legislated to use the SIN in delivering programs

and services. This has resulted in the SIN being used as the link field in many data match programs. These factors must be weighed when requested to provide the SIN number as a pure data element. Reference can be made to the TB manual on Privacy and Data Protection volume and to the Report of the Auditor General of Canada Chapter 16 September 1998 in particular 16.25 - 16.28.

- Since 1976, when the first data sharing agreement was entered into the collection, retention and distribution methods for such data has undergone tremendous change. ISP may wish to consider alternative methods in light of the technology available today. Some alternative methods include:

  => Providing access to our data by the Internet and employing security techniques such as Public Key Infrastructure (PKI). PKI is a method which allows the access to encrypted by providing a decryption key which must be matched with the host to allow for decryption;

  => Having the client provide us with their data, allowing us to conduct the match;

  => Providing a real time link to our mainframe systems for interactive searches as Insurance is doing with a limited number of screens.

External Issues for ISP:

- The organization who wishes to conduct a data match program must state the purpose of the match program and demonstrate that the program is directly related to an activity or operating program of the organization. The organization must show how they plan to use the data being shared. This should include what data elements they plan to do a match on and what the intended results will be. The match program and use of the data should be subject to approval by ISP prior to releasing the data. TB manual - Privacy and Data Protection volume 2-5 Data Matching (b) This requirement should be built into the agreement between ISP and the organization wishing to establish a matching program.

- The agreement should contain a clause which restricts the data obtained under one agreement from being used or linked in any way with the data obtained by the same organization under a separate agreement. Should such an event occur, this could potentially violate the policy on the use of personal information, limiting the use of such information for the purposes for which it was obtained. Reference to the Privacy Act; TB manual - Privacy and Data Protection 2-4 (1-2).

- Only the information that is being requested and is deemed necessary for the match program should be provided to the organization requesting the information. As stated in the HRDC Profile of Personal Information Collection, Use and Disclosure Report of 1998, this is being done however, any policy directive should re-emphasize this fact.

- The agreement should contain a clause which states that the data being shared is for a specific data match program and should be considered to remain under ISPs ownership. The agreement should restrict the contractee from further distribution or sharing of the data being requested. As mentionned above, further sharing of the data could violate the Privacy Act restricting the use of personal information for the purpose in which it was collected. TB manual 2-04-2.

- It should be established who the owner of the information is once the match is completed, for example ISP, the other organization or jointly. It should be stated in the agreement if the generated information can be shared, and if so to whom and under what circumstances it can be shared. Although we did not link this to any specific clause in the TB manual or Privacy Act, it is our opinion that this is the intent of the guidelines as outlined in the TB manual.

- The details of the match program must indicate the start and completion dates of the match program and indicate if any updates to the data being used will be required, and if so, at what intervals the updates will occur. This will ensure the data is up to date and is used effectively. TB manual - 2-5 (g). This will enable the monitoring of the match program and assist in the detection of any potential misuses by providing a clear time line which can be used in an audit.

- A time frame should be established in all agreements which will allow for the cancellation of or automatic review of the agreement on a routine basis. This built in monitoring feature will help to ensure that complacency does not occur over time regarding the sharing of information. This will also allow for changes in the match program to occur based on changing technology.

- A clause should be included in the agreements which will allow for the Minister to appoint a mutually acceptable Auditor to periodically conduct reviews and audits.

- It should be determined to what extent the regulations pertaining to the retention and subsequent disposal of the data could and should apply to the shared data. A provision which states what these regulations are should be included in the agreement. TB manual 2-03.

Income Security Programs (ISP) Data Matching/Sharing -
Security of Information & Privacy

Request: Assistance in developing related policies and guidelines and establishing an audit framework.

Background: Since 1976, ISP has entered into 30 information sharing agreements.

Many agreements have not been reviewed since signed, nor do they have a termination clause.

ISP is concerned about sharing sensitive information or information obtained from other sources such as Canada Customs and Revenue Agency (CCRA), formerly known as Revenue Canada.

Ontario implemented a co-payment program for prescription drugs based on income. Eleven residents claimed that ISP had passed on CCRA information to the province. Although this was not the case, the program had to be terminated.

Solutions: Analysis of current policies with respect to privacy, data match programs and access to information.

Development of recommendations based on internal and external ISP issues.

Details:

Internal: Creation of a data dictionary:

- Owner of data;
- Which elements may be shared;
- With whom;
- Conditions.

Awareness of the use of the social insurance number (SIN) and the Office of the Auditor General of Canada (OAG) report.

Alternatives to data sharing were suggested given advancement in technology since 1976:

- Public key infrastructure (PKI);
- ISP conducting data match with client supplied data;
- Limited direct access to our databases.

External: Development of a well written agreement stating:

- Purpose of the match program;
- How the request is directly related to their operations;

- Data shared under one agreement may not be shared with data from another match program;
- Shared data remains under the ownership of ISP;
- the Minister may appoint a mutually acceptable auditor.

The owner of the information derived from the match program and the potential use of such information should be disclosed prior to signing a data sharing agreement.

Issues pertaining to the retention and disposal of the shared data should be assessed for both federal and provincial compliance.

Outcome: Positive acceptance of the report.

Many points were new to ISP such as the creation of the data dictionary

Other points provided assurance that ISP was proceeding in the right direction.

Project was deemed complete however the door was left open if further information is needed at a later date.

Policy Objectives - Privacy and Data Protection

It is the policy of the government:

◊ to account for and give public notice of data matching carried out by or on behalf of the government; and

◊ to prevent the SIN from becoming a universal identifier by:

- limiting collection and use of the SIN by institutions to specific acts, regulations and programs, and
- notifying individual clearly as to the purposes for collecting the SIN and whether any right, benefit or privilege could be withheld or any penalty imposed if the number is not disclosed to the federal institution requesting it.

Chapter 1

Policy Requirements

Use of the Social Insurance Number

17.1 limit their uses of the Social Insurance Number (SIN) for administrative purposes to those authorized by statute or regulation and for administering pensions, income tax, health and social programs (as listed in Chapter 3-4).

17.4 when the SIN is included in any personal information bank, so indicate in the description of the bank provided for Info Source and cite the authority under which the number is collected and the purpose for which it is used.

Chapter 2

Use and Disclosure of Personal Information

Provinces, foreign states and international bodies

6.6 … information may be disclosed under an agreement … between the Government of Canada … and the government of a province … or any institution of any such government or organization, for the purpose of administering or enforcing any law …

… this permits federal government institutions to disclose personal information …for the purpose of administering a statute … Examples of this type of disclosure include the federal-provincial exchange of information related to social assistance…

Disclosures …are to be made…with a formal written agreement…these agreements must contain the components listed in Chapter 3-5.

Programmes de la sécurité du revenu
Couplage/partage des données - Sécurité de l'information et des renseignements personnels

Lignes directrices de la politique et cadre de vérification

En février 1998, toutes les ententes des PSR en vigueur sur le partage de l'information avec les provinces et les autres organismes et programmes fédéraux ont fait l'objet d'un examen. Dans tous les cas, les rapports ont indiqué que seuls les éléments des renseignements personnels qui devaient être divulgués conformément aux textes d'autorisation pertinents l'ont été. En outre, jamais une copie complète des bases de données n'a été transmise.

Le Manuel du CT - Protection des renseignements personnels énonce une série de lignes directrices relativement aux programmes de partage et de couplage des données. Il serait alors opportun d'élaborer une politique qui préciserait quelle information peut être partagée et dans quelles circonstances. Une telle politique sauvegarderait l'information personnelle sous la gouverne des PSR et en même temps, de telles politiques et des ententes ultérieures constitueraient un cadre qui permettrait d'effectuer une vérification de conformité si une telle vérification devenait nécessaire.

Aux fins du présent document :

Données - désigne une série ou des séries de documents contenant des renseignements

Programme de couplage - désigne un mécanisme particulier conçu pour servir à la comparaison des données d'une institution avec celles d'une autre.

Renseignements - désigne le produit d'un programme de couplage

Politique relative à un cadre de vérification

Questions internes pour les PSR :

- La constitution d'un dictionnaire de données qui indiquerait chaque champ de données unique contenu dans tous les systèmes et bases de données des PSR représenterait une ressource utile pour des ententes éventuelles. Pour optimiser les avantages d'un tel dictionnaire, il conviendrait que les données provenant d'autres ministères gouvernementaux, tel que l'Agence des douanes et du revenu du Canada, y soient également versées. Voici les renseignements qui seraient utiles pour un tel dictionnaire : l'identité du titulaire des données, les éléments qui peuvent être partagés, avec qui et dans quelles circonstances. Par exemple, il peut arriver que si un élément de données en particulier est considéré comme partageable, en choisissant cet élément, vous pourriez rendre non partageable un autre élément partageable. Autrement dit, les éléments de données A et B sont partageables, mais A et B ne peuvent pas

être partagés dans un même programme de couplage. Ce dictionnaire pourrait se révéler un instrument utile dans toute vérification.

- Le gouvernement a pour principe d'empêcher que le NAS ne devienne un élément d'identification universel. Cependant, les gouvernements provinciaux ont adopté des lois concernant l'utilisation du NAS dans le cadre de l'exécution de programmes et de la prestation de services. Il en a résulté que le NAS est utilisé comme champ charnière pour de nombreux programmes de couplage. Il faut tenir compte de ces facteurs lorsque le NAS est demandé à titre de simple élément de données. Pour plus de précisions, consulter le Manuel du CT - Protection des renseignements personnels et le Rapport du vérificateur général, chapitre 16, septembre 1998 et en particulier les clauses 16.25 à 16.28.

- Depuis 1976, année où la première entente de partage de données a été conclue, les méthodes de collecte, de conservation et de diffusion des données ont beaucoup changé. Les PSR voudront peut-être envisager d'autres méthodes à la lumière de la technologie disponible aujourd'hui. Voici quelques-unes des méthodes de rechange :

  ⇒ Donner accès à nos données dans Internet et à l'aide de techniques de sécurité comme l'infrastructure à clés publiques (ICP). La méthode ICP donne accès à des données chiffrées au moyen d'une clé de déchiffrage qui doit correspondre à celle de l'hôte.

  ⇒ Demander au client de nous fournir ses données pour nous permettre d'effectuer le couplage.

  ⇒ Fournir un lien en temps réel avec notre ordinateur central aux fins de la conduite de recherches interactives, comme le fait Assurance, avec un nombre limité d'écrans.

Questions externes pour les PSR :

- L'organisme qui désire exécuter un programme de couplage de données doit indiquer l'objet de ce programme de couplage et démontrer que celui-ci est relié directement à une activité ou à un programme opérationnel de l'organisme. L'organisme doit démontrer aussi comment il entend utiliser les données qui sont partagées. Il doit notamment indiquer les éléments des données qu'il prévoit apparier et le résultat qu'il en escompte. Le programme de couplage et l'utilisation des données devraient être soumis à l'approbation des PSR avant que les données ne soient divulguées. Le Manuel du CT - Protection des renseignements personnels, volume 2-5, Couplage des données (b). Cette exigence doit faire partie de l'entente passée entre les PSR et l'organisme qui désire établir un programme de couplage.

- L'entente doit contenir une clause interdisant l'utilisation ou le couplage de données obtenues au titre d'une entente de quelque façon que ce soit avec des données que le même organisme se sera procurées en vertu d'une autre entente. Une telle façon de faire risquerait d'enfreindre la politique sur l'utilisation des renseignements personnels, qui limite l'utilisation de tels renseignements aux fins pour lesquelles elles ont été obtenues. Voir *Loi sur la protection des*

renseignements personnels; Manuel du CT - Protection des renseignements personnels 2-4 (1-2).

- Seuls les renseignements demandés et qui sont jugés nécessaires pour le programme de couplage devraient être transmis à l'organisme qui les sollicite, comme il est indiqué dans le rapport sur les modalités de collecte, d'utilisation et de communication de renseignements personnels de DRHC de 1998; cependant, toute directive d'orientation devrait le rappeler.

- L'entente devrait contenir une clause qui précise que les données partagées visent un programme de couplage de données particulier et continuent d'appartenir aux PSR. L'entente doit interdire à l'exécutant de diffuser ou de partager les données demandées. Comme il est indiqué ci-dessus, tout autre partage des données risquerait d'aller à l'encontre de la *Loi sur la protection des renseignements personnels* qui limite l'utilisation des renseignements personnels aux fins pour lesquelles elles ont été recueillies, Manuel du CT 2-04-2.

- Il faudrait déterminer qui est le propriétaire de l'information une fois le couplage terminé, par exemple, les PSR, l'autre organisme, ou les deux conjointement. Il devrait être précisé dans l'entente si les renseignements produits peuvent être partagés et, dans l'affirmative, avec qui et dans quelles circonstances. Bien que ceci ne soit relié à aucune clause particulière du Manuel du CT ou de la *Loi sur la protection des renseignements personnels*, nous sommes d'avis que c'est là l'intention des lignes directrices énoncées dans le Manuel du CT.

- La description du programme de couplage doit indiquer les dates du début et de la fin du programme de couplage et préciser si des mises à jour des données utilisées seront requises et, dans l'affirmative, les intervalles auxquelles ces mises à jour auront lieu. Ainsi, les données seront à jour et utilisées efficacement. Manuel du CT - 2-5(g). Il sera ainsi possible d'assurer une surveillance au programme de couplage et de mieux détecter tout emploi abusif en fournissant une ligne temporelle claire que l'on peut utiliser dans le cadre d'une vérification.

- Pour toute entente, un échéancier devrait être établit afin de permettre l'annulation ou une révision automatique de l'entente. Cette mesure de surveillance intégrée permettra d'éviter qu'une nonchalance ne s'installe avec le temps relativement au partage des renseignements. Cela permettra également d'adapter le programme de couplage aux changements technologiques.

- Il faudrait inclure une clause dans les ententes pour permettre au Ministre de nommer un vérificateur mutuellement acceptable qui aurait charge d'effectuer régulièrement des examens et des vérifications.

- Il faudrait déterminer la mesure dans laquelle les règlements relatifs à la conservation et à l'élimination subséquente des données pourraient et devraient s'appliquer aux données partagées. Une disposition qui précise la nature de ces règlements devrait être insérée dans l'entente. Manuel du CT 2-03.

Couplage/partage des données dans le cadre des programmes de sécurité du revenu (PSR) - Sécurité de l'information et protection des renseignements personnels

Demande : Appui à l'élaboration de politiques et de lignes directrices connexes et à la mise sur pied d'un cadre de vérification.

Contexte : Depuis 1976, 30 ententes d'échange de renseignements ont été conclues dans le cadre des PSR.

Plusieurs ententes n'ont pas été révisées depuis leur signature et ne comprennent aucune clause de résiliation.

Les responsables des PSR s'interrogent sur le partage d'information de nature délicate ou de renseignements obtenus d'autres sources telles que l'Agence des douanes et du revenu du Canada (ADRC), connu anciennement sous le nom de Revenu Canada.

L'Ontario a créé un programme de remboursement partagé pour les médicaments délivrés sur ordonnance, qui repose sur le revenu. Onze résidents ont allégué que les PSR ont communiqué à la province des renseignements provenant de l'ADRC. Bien que ceci n'ait pas eu lieu, on a dû mettre fin au programme.

Solutions : Analyse des politiques existantes liées à la protection des renseignements personnels, aux programmes de couplage de données et à l'accès à l'information.

Formulation de recommandations à partir des questions internes et externes relatives aux PSR.

Détails :

Questions internes : Création d'un dictionnaire de données :

- identité du titulaire;
- éléments pouvant être partagés;
- avec qui;
- conditions.

Sensibilisation quant à l'usage du numéro d'assurance sociale (NAS) et du rapport du Bureau du vérificateur général (BVG) du Canada.

Vu les progrès réalisés dans le domaine de la technologie depuis 1976, des solutions de rechange pour le partage de données ont été proposées :

- Infrastructure à clés publiques (ICP);
- Les PSR effectuent le couplage à partir de données fournies par le client;
- Accès direct et limité à nos bases de données.

Questions externes :

Élaboration d'une entente bien rédigée précisant :

- L'objet du programme de couplage;
- En quoi la demande est directement liée aux opérations;
- Les données partagées dans le cadre d'une entente ne peuvent être partagées avec des données obtenues par l'intermédiaire d'un autre programme de couplage;
- Les données partagées sont la propriété des PSR;
- La Ministre peut nommer un vérificateur mutuellement acceptable.

Le titulaire de données provenant du programme de couplage et l'usage potentiel de ces données doivent être établis avant la signature d'une entente de partage de données.

Les questions relatives à la conservation et à l'élimination des données partagées devraient être évaluées conformément aux lois fédérales et provinciales.

Résultats : Accueil positif vis-à-vis le rapport.

Plusieurs questions étaient nouvelles pour les PSR, telles que la création d'un dictionnaire de données.

D'autres éléments ont confirmé que les PSR étaient dans la bonne direction.

Le projet est considéré comme terminé. Il est toutefois possible qu'on s'y réfère à une date ultérieure.

Objectifs de la politique sur la Protection des renseignements personnels

La politique du gouvernement est la suivante :

◊ tenir compte et faire état du couplage des données effectué par le gouvernement ou en son nom;

◊ éviter que le NAS ne devienne un identificateur universel et, à cette fin, prendre les mesures suivantes :

- restreindre à des lois, des règlements et des programmes précis la collecte et l'utilisation du NAS par les institutions;

- informer clairement les personnes concernées des fins auxquelles leur NAS est recueilli ainsi que des droits, avantages ou privilèges qui pourraient leur être retirés ou des sanctions qui pourraient leur être imposées si elles refusent de divulguer leur numéro à une institution fédérale qui en fait la demande.

Chapitre 1

Exigences

Utilisation du numéro d'assurance sociale

17.1 Restreindre l'utilisation du numéro d'assurance sociale (NAS) aux fins autorisées par une loi ou un règlement et pour l'administration des pensions, de l'impôt sur le revenu ainsi que des programmes sociaux et de santé (selon le chapitre 3-4).

17.4 Quand le NAS est versé dans un fichier de renseignements personnels, l'institution fédérale doit le signaler dans la description du fichier à être inclue dans Info Source et citer l'autorité en vertu de laquelle le numéro a été recueilli ainsi que les fins auxquelles il est utilisé.

Chapitre 2

Usage et communication des renseignements personnels

Provinces, États étrangers et organisations internationales

6.6 … renseignements personnels peuvent être communiqués aux termes d'accords ou d'ententes […] entre le gouvernement du Canada [...] et un gouvernement d'une province [...] ou de gouvernements, ou un de leurs organismes, en vue de l'application des lois [...].

C'et alinéa permet [...] de communiquer [...] en vue de faire appliquer ou exécuter une loi. C'est le cas par exemple des échanges fédéro-provinciaux de renseignements concernant l'aide sociale [...].

Les divulgations [...] doivent être faites [...] d'un accord ou d'une entente écrits [...] devant [...] contenir les éléments écrits au chapitre 3-5.